Tina Wolfson, CA Bar No. 174806
twolfson@ahdootwolfson.com
Theodore Maya, CA Bar No. 223242
tmaya@ahdootwolfson.com
**AHDOOT & WOLFSON, PC**
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: 310-474-9111; Fax: 310-474-8585

Daniel S. Robinson, CA Bar No. 244245
drobinson@robinsonfirm.com
Wesley K. Polischuk, CA Bar No. 254121
wpolischuk@robinsonfirm.com
**Robinson Calcagnie, Inc.**
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288
Fax: (949) 720-1292

Daniel K. Bryson (*pro hac vice* to be filed)
Dan@wbmllp.com
WHITFIELD BRYSON & MASON LLP
900 W. Morgan St.
Raleigh, NC 27603
Tel: 919-600-5000; Fax: 919-600-5035

Counsel for Plaintiffs

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO DIVISION**

STEVEN AGANS and AUDREY DIAZ SANCHEZ, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

UBER TECHNOLOGIES, INC., a Delaware Corporation, and Does 1-50

Defendant.

Case No. _____

**CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

Plaintiffs Steven Agans and Audrey Diaz Sanchez (collectively, "Plaintiffs"), by and through their counsel, bring this Class Action Complaint against Defendant Uber Technologies, Inc. ("Defendant"), on behalf of themselves and all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

## PARTIES

1. Plaintiff Steven Agans is an individual and a resident of Atlanta, Georgia, who drove for Defendant in late 2013 and early 2014.

2. Plaintiff Audrey Diaz Sanchez is an individual and a resident of Santa Barbara, California, who has used Defendant's services as a rider since approximately 2013 through 2017.

3. Defendant is a company that conducts business throughout the United States. Defendant is a corporation organized under the laws of the state of Delaware with its principal place of business at 800 Market Street, 7th Floor, San Francisco, CA 94102.

4. Plaintiffs are unaware of the true names and capacities of the defendants sued as DOES 1-50, and therefore sue these defendants by fictitious names. Plaintiffs will seek leave to amend this Complaint when and if the true identities of these DOE defendants are discovered. Plaintiffs are informed and believe and thereon allege that each of the defendants designated as a DOE is responsible in some manner for the acts and occurrences alleged herein, whether such acts or occurrences were committed intentionally, negligently, recklessly or otherwise, and that each said DOE defendant thereby proximately caused injuries and damages to Plaintiffs as herein alleged, and is thus liable for the damages suffered by Plaintiffs.

## JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2), in that the matter is a class action wherein the amount in controversy

exceeds the sum or value of $5,000,000, exclusive of interest and costs, and members of the Class are citizens of states different from Defendant.

6. This Court has personal jurisdiction over Defendant because it is headquartered and is registered to conduct business in California.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides here, and under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to this action occurred in this District.

## FACTUAL BACKGROUND

8. Plaintiffs bring this class action against Defendant for its failure to secure and safeguard their personal identifying information ("Private Information"), and that of some 57 million similarly situated people who either drove for Defendant or used its services as riders, and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their Private Information had been stolen and precisely what types of information were stolen.

9. Defendant develops, markets, and operates a mobile-app-based transportation network called Uber. The Uber app allows riders to submit a trip request on their smartphone, which is routed to Defendant's drivers.

10. Defendant's business depends on drivers, who must provide their Private Information, including extremely sensitive Private Information such as their Social Security Numbers, to Defendants in order to work as drivers and earn a livelihood.

11. Riders also must provide Private Information in order to use Uber's services, including financial information that is required to pay for rides through Defendants' App.

### A. Defendant Failed to Notify Class Members About a Massive Data Breach in 2016, Instead Paying Hackers to Cover It Up

12. On November 21, 2017, news reports were published that made it public, for the first time, that Defendant suffered a massive data breach in October 2016, in which the Private Information of some 57 million of Defendant's riders and drivers was

accessed by hackers (the "2016 Data Breach"). *See, e.g.*, <https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data> (last visited Nov. 22, 2017).

13. Defendant learned about 2016 Data Breach by November 2016, but purposely chose not to notify those whose Private Information was compromised at that time.

14. Instead of notifying the victims of the 2016 Data Breach about it, Defendant paid the hackers who perpetrated it $100,000 in an effort to cover up the 2016 Data Breach. *Id.*

15. Defendant thus conspired with the hackers who perpetrated the 2016 Data Breach to keep its victims — Defendant's drivers and riders — ignorant about it.

16. According to the news reports, the 2016 Data Breach occurred when two hackers "accessed a private GitHub coding site used by Uber software engineers and then used login credentials they obtained there to access data stored on an Amazon Web Services account that handled computing tasks for the company. From there, the hackers discovered an archive of rider and driver information. Later, they emailed Uber asking for money, according to the company." *Id.*

17. "Compromised data from the October 2016 attack included names, email addresses and phone numbers of 50 million Uber riders around the world, the company told Bloomberg on Tuesday. The personal information of about 7 million drivers was accessed as well, including some 600,000 U.S. driver's license numbers. No Social Security numbers, credit card information, trip location details or other data were taken, Uber said." *Id.*

18. According to these news reports, Defendant's board of directors commissioned an investigation into the activities of its security team in or around October 2017, which team was led by Defendant's Chief Security Officer, Joe Sullivan. This project, conducted by an outside law firm, discovered the 2016 Data Breach and the failure to disclose it. *Id.*

19. In response to this discovery, Dara Khosrowshahi, who has been Defendant's CEO since August 2017, asked for the resignation of Mr. Sullivan and fired Craig Clark, a senior lawyer who reported to Mr. Sullivan. *Id.*

20. As these news reports surfaced, Defendant published several statements concerning the 2016 Data Breach on its own website, confirming much of what was published in the news reports.

21. According to one of Defendant's statements concerning the 2016 Data Breach: "Driver information included the names, email addresses and mobile phone numbers related to accounts globally. In addition, the driver's license numbers of around 600,000 drivers in the United States were downloaded." <https://help.uber.com/h/0ded7de4-ed4d-4c75-a3ee-00cddeafc372> (last visited Nov. 22, 2017).

22. Defendant has yet to provide any direct notification to victims of the 2016 Data Breach that their Personal Information was compromised.

**B. <u>Defendant Also Failed to Notify Class Members About a 2014 Data Breach that Preceded, and Was Similar in Many Ways to, the 2016 Data Breach</u>**

23. At the time Defendant discovered the 2016 Data Breach and made the illegal and reprehensible decision not to disclose it, Defendant had recently settled a lawsuit with the New York attorney general over a very similar data breach that occurred in 2014 (the "2014 Data Breach"), and was in the process of negotiating with the Federal Trade Commission over its handling of consumer data.

24. In the 2014 Data Breach, much like the 2016 Data Breach, one or more hackers utilized credentials that Defendant made available on one or more GitHub webpages (and/or via the GitHub app, which is an app designed for sharing code among app developers). *See, e.g.*, <http://www.theregister.co.uk/2015/02/28/uber_subpoenas_github_for_hacker_details> (last visited March 11, 2015).

25. Defendant did not disclose the 2014 Data Breach until February 27, 2015, when it disseminated a Press Release stating, *inter alia*, "In late 2014, we identified a

one-time access of an Uber database by an unauthorized third party. . . .” (the “2015 Press Release”).

26. Defendant admitted in its 2015 Press Release that it knew of the 2014 Data Breach at least as early as September 17, 2014 — over five months before Defendant issued the 2015 Press Release or made any effort whatsoever to notify those affected that their Private Information had been disclosed in the Data Breach. (*Id.*)

27. Defendant’s 2015 Press Release further stated that “unauthorized access to an Uber database by a third party . . . occurred on May 13, 2014,” and that “the unauthorized access impacted approximately 50,000 drivers across multiple states.” (*Id.*)

28. At approximately the same time it issued its 2015 Press Release, Defendant also issued notifications to victims of the 2014 Data Breach, including Plaintiff Agans, which included substantially the same information and which informed recipients that their name and driver’s license numbers were disclosed in the 2014 Data Breach.

29. Defendant’s initial representations about the 2014 indicated, much as its current representations concerning the 2016 Data Breach indicate, that only drivers’ license numbers and names were disclosed in the 2014 Data Breach. However, this turned out not to be true.

30. In or around August 2016 — approximately two years after the 2014 Data Breach, and shortly before Defendant’s discovery of the 2016 Data Breach — Defendant issued more notifications to victims of the 2014 Data Breach informing them that, contrary to its earlier representations and notices, additional Private Information was disclosed in the 2014 Data Breach (the “Second 2014 Breach Notification”)

31. In its Second 2014 Breach Notifications Defendant revealed that, contrary to its initial representations concerning the scope of the 2014 Data Breach, additional Private Information was disclosed in the 2014 Data Breach, including banking information and Social Security Numbers, in addition to driver’s license numbers and

names.

**C. Plaintiffs Were Injured by the 2016 Data Breach**

32. Defendant has repeatedly disregarded Plaintiffs' and Class members' rights by intentionally, willfully, and recklessly failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the 2016 Data Breach from ever happening, despite its experience with the 2014 Data Breach (which both occurred because Defendant made credentials available through GitHub websites), and failing to disclose to those affected the facts that it did not have adequate computer systems and security practices in place, or that the Data Breach had occurred in a timely manner. On information and belief, Plaintiffs' and Class members' Private Information and the password allowing access to that Private Information were improperly handled and stored, were unencrypted, and were not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs' and Class members' Private Information was compromised and stolen.

33. Disclosure of the types of Private Information that Defendant admits were compromised in the 2016 Data Breach presents a danger to victims of the breach. Information such as data breach victims' names, birth dates, email addresses, and other identifying information *alone* creates a material risk of identity theft. Identity thieves can use such Private Information to locate additional Private Information, such as financial information and Social Security Numbers, and use the combined information to perpetrate fraud such as, for instance, opening new financial accounts in victims' names, or filing false tax returns in victims' names and collecting the tax refunds.

34. However, given the facts surrounding the 2014 and 2016 Data Breaches, Defendant's current representations concerning the scope of the 2016 Data Breach cannot be accepted as true. Defendant possesses a wide variety of Private Information concerning Class Members, and repeatedly has failed to protect that Private Information. Based on the facts alleged above, Plaintiffs assume that all the Private

Information that Defendant has about them has been handled incompetently and improperly, and Plaintiffs must assume that all of the Private Information in Defendant's possession has been obtained by hackers who either will misuse that Private Information themselves or sell it to others to who will do so, if this has not already occurred. There is no expiration on how long victims' Private Information can stay in the hands of identity thieves before it is misused.

35. Plaintiffs and other Class Members suffered injuries including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, invasion of their privacy, and loss of value of their Private Information.

36. It is well known and the subject of many media reports that Private Information like that taken in the Data Breach at issue is highly coveted and a frequent target of hackers.

37. Legitimate organizations and the criminal underground alike recognize the value in such Private Information. Otherwise, they wouldn't pay for it or aggressively seek it.

38. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." Verizon 2014 PCI Compliance Report, *available at* <http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited June 9, 2017).

39. The ramifications of Defendant's failure to keep Class members' data secure are severe.

40. There is a strong likelihood that Class members will become victims of identity fraud in the future given the breadth of their Private Information that is now available to ID thieves and other criminals on the dark web. For instance, According to a Javelin Strategy and Research Study, 16% of all Americans have been victims of identity theft as of 2016. <https://www.javelinstrategy.com/press-release/identity-fraud-

hits-record-high-154-million-us-victims-2016-16-percent-according-new> (last visited Nov. 22, 2017).

41. As the FTC recognizes, once identity thieves have Private Information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[1]

42. Identity thieves can use Private Information such as that of Class members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

43. In addition, identity thieves may get medical services using consumers' compromised Private Information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

44. Plaintiffs and other Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges that may be incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

45. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and other Class members' Private Information, causing them to suffer, and continue to suffer, economic

[1] FTC, Warning Signs of Identity Theft, *available at* <http://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited June 9, 2017).

damages and other actual harm for which they are entitled to compensation, including:

a. theft of their Private Information;

b. damage to Plaintiff's and Class members' credit reports and/or scores;

c. the untimely and inadequate notification of the Data Breach;

d. loss of privacy;

e. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. deprivation of rights they possess under California law, including the Consumer Records Act and Business and Professions Code § 17200, *et seq.*

## CLASS ACTION ALLEGATIONS

46. Plaintiffs seek relief in their individual capacity and as representatives of all others who are similarly situated. In accordance with Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiffs seek certification of a National Class, a California class, and a Georgia Class (collectively, the "Class").

47. The National Class initially is defined as follows:

> All persons residing in the United States whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2016 (the "National Class").

48. The California Class is initially defined as follows:

> All persons residing in California whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2016 (the "California Class").

49. The Georgia Class is initially defined as follows:

> All persons residing in Georgia whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2016 (the "Georgia Class").

50. Excluded from the Class are Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by

Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

51. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on Defendant's statements Private Information pertaining to approximate 57 million riders and drivers, globally, was disclosed in the Data Breach.

52. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant violated California Civil Code § 1798.81.5 by failing to implement reasonable security procedures and practices;
b. Whether Defendant violated California Civil Code § 1798.82 by failing to promptly notify class members their Private Information had been compromised;
c. Whether class members may obtain an injunctive relief against Defendant under Civil Code § 1798.84 or under the UCL;
d. What security procedures and data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;
e. Whether Defendant has an express or implied contractual obligation to use reasonable security measures;
f. Whether Defendant complied with any express or implied contractual obligation to use reasonable security measures;
g. Whether Defendant violated California Business and Professions Code § 17200, *et seq.*; and

h. The nature of the relief, including equitable relief, to which Plaintiff and the Class members are entitled.

53. Ascertainability. All members of the purposed Class are readily ascertainable. Defendant has access to addresses and other contact information for all, or substantially all, members of the Class, which can be used for providing notice to many Class members.

54. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed by Defendant.

55. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

56. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

57. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

58. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

**COUNT I**

**For Violation of the Civil Code Sections 1798.81.5 & 1798.82**

**(On Behalf of Plaintiffs and the National Class or, in the alternative, the California Class)**

59. Plaintiffs incorporate the substantive allegations above as if fully set forth herein.

60. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

61. The Private Information taken in the Data Breach fits within the definition of "Personal information" in Civil Code section 1798.80.

62. Plaintiffs and other Class members provided their personal information to Defendant in order to use the Uber App to generate income by providing services as Uber drivers, or to get rides as riders, and thus qualify as "Customer[s]" as defined in Civil Code section 1798.80.

63. Defendant failed to dispose of Plaintiffs' Private Information after they no longer were working as Uber drivers or using the Uber App as riders, allowing that Private Information to be compromised in the 2016 Data Breach and violating Civil Code section 1798.81.

64. By failing to implement reasonable measures to protect the Private Information in its possession, Defendant violated Civil Code section 1798.81.5.

65. In addition, by failing to promptly notify all who were affected by the 2016 Data Breach that their Private Information had been acquired (or was reasonably believed to have been acquired) by hackers, Defendant violated Civil Code Section 1798.82.

66. As a direct or proximate result of Defendant's violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Plaintiff and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in this Class Action Complaint.

67. Defendant's violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82 were, at a minimum, reckless.

68. In addition, by violating Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Defendant "may be enjoined" under Civil Code Section 1798.84(e).

69. Defendant's violations of Civil Code Section 1798.81.5 and 1798.82 also constitute an unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 *et seq.*, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

70. Plaintiffs accordingly request that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption algorithms for encryption keys that provide access to stored Private Information; (2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's computer system is compromised, hackers cannot gain access to other portions of its systems; (7) ordering that Defendant purge, delete, destroy in a

reasonable secure manner customer data not necessary for its ongoing relationship with drivers; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to drivers; (10) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (11) ordering that Defendant stop using GitHub or allowing Private Information to be accessed with single credentials; and (12) ordering Defendant to meaningfully educate its drivers and riders about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

71. Plaintiffs further request that the Court require Defendant to identify and notify all members of the Class who have not yet been informed of the Data Breach, and to notify affected drivers and/or users of its app of any future data breaches by email within 24 hours of Defendant's discovery of a breach or possible breach and by mail within 72 hours.

72. Plaintiffs and the Class are entitled to actual damages in an amount to be determined at trial under Civil Code Section 1798.84.

73. Plaintiffs and the Class also are entitled to an aware of attorney fees and costs under Civil Code Section 1798.84.

## COUNT II

**Violation of California Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq*.**

**(On Behalf of Plaintiffs and the National Class or, in the alternative, the California Class)**

74. Plaintiffs incorporate the substantive allegations above as if fully set forth herein.

75. Defendant engaged in unfair, fraudulent and unlawful business practices in

violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL").

76. Plaintiffs suffered injury in fact and lost money or property as a result of Defendant's alleged violations of the UCL.

77. The acts, omissions, and conduct of Defendant as alleged constitutes a "business practice" within the meaning of the UCL.

78. Defendant violated the unlawful prong of the UCL by violating Civil Code Sections 1798.81.5 and 1798.82, as alleged above.

79. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and other Class members. The harm cause by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

80. Defendant's conduct also undermines California public policy — as reflected in statutes like the Information Practices Act, Cal. Civ. Code § 1798 *et seq.*, and the California Customer Records Act, Cal. Civ. Code §§ 1798.81.5 and 1798.82 concerning customer records — which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

81. By failing to disclose that it does not enlist industry standard security practices, which render Defendant's app and services particularly vulnerable to data breaches, Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

82. A reasonable person would not have agreed to use the Uber app or to act as an Uber driver had he or she known the truth about Defendant's security procedures. By withholding material information about Defendant's security practices, it was able to

convince drivers and riders to provide and entrust their Private Information to Defendant.

83. Defendant's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to Class members.

84. As a result of Defendant's violations of the UCL, Plaintiff and the other Class members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption algorithms for encryption keys that provide access to stored Private Information; (2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment Private Information by, among other things, creating firewalls and access controls so that if one area of Defendant's computer system is compromised, hackers cannot gain access to other portions of its systems; (7) ordering that Defendant purge, delete, destroy in a reasonably secure manner Private Information not necessary for its provisions of services; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate smartphone and web applications for vulnerabilities to prevent threats to drivers and other users of the Uber app; (10) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and

education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (11) ordering that Defendant stop using GitHub or allowing Private Information to be accessed with single credentials; and (12) ordering Defendant to meaningfully educate its drivers and riders about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

85. As a result of Defendant's violations of the UCL, Plaintiff and other Class members have suffered injury in fact and lost money or property, as detailed above. Plaintiff requests that the Court issue sufficient equitable relief to restore Class members to the position they would have been in had Defendant not engaged in unfair competition, including by ordering restitution of all funds that Defendant acquired as a result of its unfair competition, including fees that Defendant retained for rides given by Plaintiff and other Class members.

## COUNT III

### Negligence

**(On Behalf of Plaintiffs and the National Class or, in the alternative, the California Class and the Georgia Class)**

86. Plaintiffs incorporate the substantive allegations above as if fully set forth herein.

87. Defendant owed a duty to Plaintiffs and Class members, who were required to provide their Private Information to Defendant in order to get paid for their work as Uber drivers, arising from the sensitivity of the Private Information and the foreseeability of the 2016 Data Breach and of Defendant's data security shortcomings, to exercise reasonable care in safeguarding their Private Information. This duty included, among other things, designing, maintaining, implementing, monitoring, testing, and complying with reliable security systems, protocols, and practices to ensure that Class members' information adequately secured from unauthorized access.

88. Defendant owed a duty to Class members to implement cybersecurity

systems and processes that would detect a data breach in a timely manner, and not allow Private Information or keys that would access Private Information to be published or otherwise made available to identity thieves.

89. Defendant also had a duty to delete any Private Information that was no longer needed to serve its drivers' and riders' needs, and not use former drivers' or riders' Private Information in the conduct of its business going forward.

90. Defendant also owed a duty to Class members to notify them promptly that their Private Information was compromised in the 2016 Data Breach.

91. Defendant breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class member' Private Information; (b) failing to detect the Data Breach in a timely manner; (c) filing to notify Class membrs promptly and with full information concerning the Data Breach; and (d) failing to disclose that Defendants' data security practices were inadequate to safeguard Class member' Private Information.

92. But for Defendant's breach of its duties, Class member' Private Information would not have been compromised in the Data Breach.

93. Plaintiffs and Class member were foreseeable victims of Defendant's inadequate data security practices. Defendant knew or should have known that a breach of its data security systems would cause damages to Class members.

94. As a result of Defendant's negligent and/or willful failure to prevent the Data Breach, Plaintiffs and Class member suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class member must more closely monitor their financial accounts and credit histories to guard against identity theft and mis-use of their Private Information. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized release of Plaintiffs' and Class member' Private Information also

diminished the value of that Private Information.

95. The damages to Plaintiffs and other Class members were a proximate, reasonably foreseeable result of Defendant's breaches of its duties.

96. Plaintiffs and Class member are entitled to damages in an amount to be proven at trial.

**COUNT III**

**VIOLATION OF THE GEORGIA FAIR BUSINESS PRACTICES ACT**

**Ga. Code Ann. § 10-1-390, *et seq*.**

**(On Behalf of Plaintiff Agans and the Georgia Subclass)**

97. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

98. Defendant, while operating in Georgia, engaged in unfair and deceptive consumer acts in the conduct of trade and commerce, in violation of Ga. Code Ann. § 10-1-390(a), and (b). This includes but is not limited the following:

a. Defendant failed to enact adequate privacy and security measures to protect the Georgia Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the 2016 Data Breach;

b. Defendant failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the 2016 Data Breach;

c. Defendant knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Georgia Class members' Private Information from unauthorized disclosure, release, data breaches, and theft;

d. Defendant knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for the Georgia Class members' Private Information;

e. Defendant failed to maintain the privacy and security of Georgia Class members' Private Information, in violation of duties imposed by applicable federal and state laws, which was a direct and proximate cause of the 2016 Data Breach; and

f. Defendant failed to disclose the 2016 Data Breach to Georgia Class members in a timely and accurate manner, in violation of § Ga. Code Ann 10-1-912.

99. As a direct and proximate result of Defendant's practices, Georgia Class members suffered the injury and/or damages described herein, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information.

100. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Georgia Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

101. Defendant knew or should have known that its systems and practices, including its use of GitHub, were inadequate to safeguard Georgia Class members' Private Information, and that the risk of a data breach or theft was highly likely. Defendant's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of Georgia Class members.

102. Plaintiffs and the Georgia Class seek damages and treble damages (for intentional violations), to be proven at trial, under Ga. Code. Ann. § 10-1-399(a) and (c).

103. Plaintiffs also seek an order enjoining Defendant's unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under Ga. Code. Ann. § 10-1-399.

## REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to its data collection, storage, and safety practices and to disclose with specificity to Class members the type of data compromised in the 2016 Data Breach, and other information required under Cal. Civ. Code § 1798.82;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

## DEMAND FOR JURY TRIAL

Plaintiffs demand trial by jury of all claims so triable.

Dated: November 22, 2017

Respectfully submitted,

**AHDOOT & WOLFSON, PC**

Tina Wolfson
Robert Ahdoot
Theodore W. Maya
Bradley King
Keith Custis (Of Counsel)
**AHDOOT & WOLFSON, PC**
10728 Lindbrook Dr.
Los Angeles, California 90024
Telephone: 310-474-9111
Facsimile: 310-474-8585

Daniel S. Robinson, CA Bar No. 244245
drobinson@robinsonfirm.com
Wesley K. Polischuk, CA Bar No. 254121
wpolischuk@robinsonfirm.com
**Robinson Calcagnie, Inc.**
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288
Fax: (949) 720-1292

Daniel K. Bryson (*pro hac vice* to be filed)
Dan@wbmllp.com
**WHITFIELD BRYSON & MASON LLP**
900 W. Morgan St.
Raleigh, NC 27603
Tel: 919-600-5000; Fax: 919-600-5035

*Counsel for Plaintiffs*